



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

July 6, 2009

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

ADVISORY NUMBER:
SA2009-030 UPDATED

DATE(S) ISSUED:
7/6/2009

7/9/2009 - **UPDATED**

SUBJECT:
Vulnerability in FCKEditor Could Allow For Remote Code Execution

ORIGINAL OVERVIEW:
A vulnerability has been identified in FCKEditor that could allow for remote code execution. FCKEditor is a standalone HTML text editor application that may be bundled with other commonly used applications. This vulnerability can be exploited by using the 'connector.php' script to upload content to the hosting webserver. Successful exploitation may result in an attacker gaining the same privileges as the webserver process. Depending on the privileges associated with the webserver process, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in denial-of-service conditions.

It should be noted that this vulnerability is being actively exploited on the Internet.

JULY 9 UPDATED OVERVIEW:

Adobe has released a HotFix and FCKEditor has published an update for this issue.

SYSTEMS AFFECTED:

- Alexscriptengine Article-Engine 1.3.0
- Alexscriptengine News-Engine 1.5.1
- Falt4 CMS Falt4 Extreme RC4
- FCKeditor FCKeditor 2.0.0 rc2

- FCKeditor FCKeditor 2.0.0 rc3
- FCKeditor FCKeditor 2.2
- FCKeditor FCKeditor 2.3 beta
- FCKeditor FCKeditor 2.4.3
- FCKeditor FCKeditor 2.6.4
- PHPList PHPList 2.10.1
- PHPList PHPList 2.10.2
- PHPList PHPList 2.10.3
- PHPList PHPList 2.10.4
- PHPList PHPList 2.10.5
- PHPList PHPList 2.10.6
- Tru-Zone NukeET 3.4
- Oracle Application Express 3.0 or greater
- Oracle 11g
- Oracle 10g Release 2
- ColdFusion 8 or greater

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

ORIGINAL DESCRIPTION:

A vulnerability has been identified in FCKEditor that could allow for remote code execution. The vulnerability is triggered by using the 'connector.php' script to upload content to the webserver. When uploading a specified file type the application fails to verify that the content within the file matches that particular file type (i.e. A Microsoft Word file is specified to be uploaded but a perl script is uploaded in its place). There are known exploits available.

Successful exploitation may result in an attacker gaining the same privileges as the webserver process on the server. Depending on the privileges associated with the webserver process, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploitation could result in denial-of-service conditions.

To remediate this issue, it is recommended to remove the 'connector.php' script and update to FCKEditor 2.6.4.1 or if FCKEditor was not installed separately but instead integrated as part of another application then apply that vendor's update.

ColdFusion recommends as a best practice to turn off the connector. However, if the connector cannot be turned off due to business requirements, it is possible to reduce the risk by moving the directory where the connector is located to a non-standard location.

The application of standard security practices regarding folder permissions as well as the detailed examination of uploaded files will also help in greatly reducing the risk of compromise.

Be aware that even though this application has typically been associated with PHP and ColdFusion, it is available for ASP.Net, ASP, Java, Active-FoxPro, Lasso, Perl, and Python.

It should be noted that this vulnerability is being actively exploited on the Internet.

JULY 9 UPDATED Description:

The Adobe HotFix addresses the vulnerability in FCKEditor referenced in this advisory. It is worth noting that Adobe ColdFusion version 8 is not susceptible to this exploit unless the cfm connectors configuration file has been modified from the default value to allow file uploads. The Adobe HotFix also updates the version of FCKEditor, so separate patching for that software is unnecessary.

ORIGINAL RECOMMENDATIONS:

We recommend the following actions be taken:

- Remove the connector and install the appropriate vendor's update as soon as it becomes available after appropriate testing.
- Apply the principle of Least Privilege to all services.
- See description above for workarounds.
- Ensure that all anti-virus software is up to date with the latest signatures.

July 9 UPDATED RECOMMENDATIONS:

- Apply the new patches to vulnerable systems immediately after appropriate testing.
- Consider applying the workarounds recommended by the vendor immediately after appropriate testing.

ORIGINAL REFERENCES:

Security Focus:

<http://www.securityfocus.com/archive/1/20090703154521.GY6089@inversepath.com>

oCERT:

<http://www.ocert.org/advisories/ocert-2009-007.html>

FCKEditor:

<http://www.fckeditor.net/>

SANS:

<http://isc.sans.org/diary.html?storyid=6715>

July 9 UPDATED REFERENCES:

FCKEditor:

<http://www.fckeditor.net/whatsnew>

Adobe ColdFusion:

<http://www.adobe.com/support/security/bulletins/apsb09-09.html>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2265>

Security Focus:

<http://www.securityfocus.com/bid/31812>